

1

**System and Method for Multiple Virtual
Private Network Authentication Schemes**

ABSTRACT

A system and method for providing multiple virtual
5 private networks from a computer system. The computer
system communicates with a remote computer system in order
to allow encrypted data traffic to flow between the
respective systems. Two phases are used to authenticate
the computer systems to one another. During the first
10 phase, digital certificates or pre-shared keys are used to
authenticate the computer systems. A phase 1 ID rules list
contains authentication rules for local-remote computer
pairs. During the second phase, a hash value is used to
authenticate the computer systems and a security
15 association payload is created. The remote system's IP
address is used for connecting. The phase 1 ID rules list
corresponds to one or more phase 2 ID rules lists. If the
remote ID is not found in the phase 2 ID rules list, a
default rule is used based upon the phase 1 ID rules list.